The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
11/9/2009

SUBJECT:
Vulnerability in TLS Protocol Session Renegotiation

OVERVIEW:
A vulnerability exists in the Transport Layer Security (TLS) protocol that could allow attackers to intercept secure communications from unsuspecting users. TLS is widely used to provide secure communication over the Internet. If successfully exploited, this could result in information disclosure or credential theft of the affected user.

Please note: Proof of concept code has been published and is publically available. However, we have not received any reports of active exploitation of this vulnerability.

SYSTEMS AFFECTED:

Apache Software Foundation Apache 2.2.8
Apache Software Foundation Apache 2.2.9
GNU GnuTLS 2.0.0 - 2.8.3
Microsoft IIS 7.0
Microsoft IIS 7.5
OpenSSL Project OpenSSL 0.9.8h and prior
MandrakeSoft Multi Network Firewall 2.0
MandrakeSoft Linux Mandrake 2009.0 - 2009.1
MandrakeSoft Enterprise Server 4.0 - 5.0
MandrakeSoft Corporate Server 3.0 - 5.0

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in the Transport Layer Security (TLS) protocol that could allow attackers to perform man-in-the-middle (MITM) attacks. TLS provides secure communication for a variety of applications over the Transport layer. This vulnerability is known to work with the Hypertext Transport Protocol (HTTP), but is believed to be applicable to any other protocol that utilizes TLS for security. In the example of HTTP, the attack is performed by intercepting the 'Client Hello' and forcing

the current TLS session to renegotiate the cipher used to secure the communications between hosts. This request for a new cipher is not made over the encrypted channel, but made in plaintext. In addition, to save time, Session ID's can be reused for the renegotiation process, thereby permitting easier exploitation by the attacker.

Successful usage of a MITM attack to exploit this issue does not allow for the decryption of the data, but does allow for the attacker to inject specifically crafted packets in the context of the current session. Also, it is of note to state that once a successful MITM attack has been executed that tools do exist to decrypt the traffic being controlled by the attacking host.

Please note: Proof of concept code has been published and is publically available. However, we have not received any reports of active exploitation of this vulnerability.

Multiple vendors have released patches that address this vulnerability.

RECOMMENDATIONS:

The following actions should be taken:

- Apply the appropriate vendor patches to vulnerable systems as soon as it becomes available after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- If you believe you have been affected by attacks exploiting this vulnerability, please contact us immediately.

REFERENCES:

Secunia:
http://secunia.com/advisories/37291/
http://secunia.com/advisories/37292/

Security Focus:
http://www.securityfocus.com/bid/36935

Sun:
http://blogs.sun.com/security/entry/vulnerability_in_tls_protocol_during

OpenSSL:
http://cvs.openssl.org/chngview?cn=18790
http://www.openssl.org/source/openssl-0.9.8l.tar.gz

MandrakeSoft:
http://www.mandriva.com/en/download/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555